



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11340968 A**(43) Date of publication of application: **10.12.99**

(51) Int. Cl. **H04L 9/32**  
**G09C 1/00**  
**G09C 1/00**

(21) Application number: **10145284**(22) Date of filing: **27.05.98**(71) Applicant: **MITSUBISHI ELECTRIC CORP**(72) Inventor: **SAKAKIBARA HIROYUKI**  
**YOSHITAKE ATSUSHI**(54) **INVALID INFORMATION VERIFICATION SYSTEM**

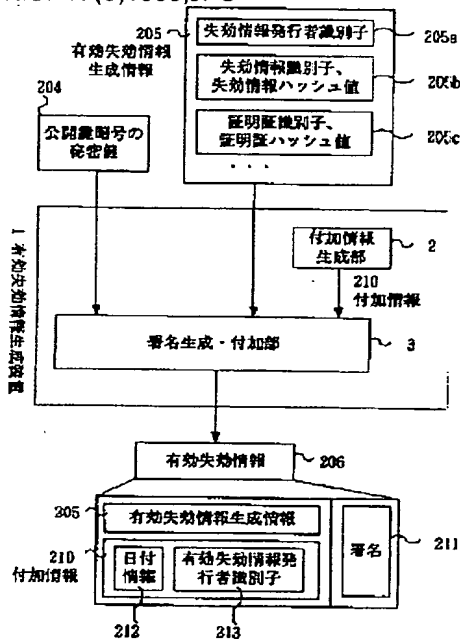
## (57) Abstract:

**PROBLEM TO BE SOLVED:** To reduce processing to verify the information denoting that a certificate is invalid.

**SOLUTION:** The system is provided with an additional information generating section 2 that generates additional information 210 consisting of date information 212 denoting the validity of valid-invalid information 206 for verifying the information, a valid-invalid information issuing party identifier 213, a signature generating addition section 3 that receives one set of combinations of an identifier 205a of an invalid information issuing party. A set or more of an identifier 205b of invalid information, an invalid information hash value 205b, an identifier 205c for a certificate for verifying the information to verify a signature of the invalid information, and a hash value 205c for the invalid information verification certificate are inputted. These input data with the additional information 210 generated by the additional information generating section 2 are merged, a signature 211 by a secret key 204 of a public key encryption held by a management agent for the invalid information is added to the merged data. The system is also provided

with a signature generating and adding part 3 for the valid invalid information.

COPYRIGHT: (C)1999, JPO





(19) 日本国特許庁 (JP)

# (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 11 - 340968

(43) 公開日 平成 11 年 (1999) 12 月 10 日

(51) Int. Cl. °

識別記号

F. I

H 0 4 L 9/32

G 0 9 C 1/00

6 2 0

6 4 0

H 0 4 L 9/00

G 0 9 C 1/00

6 7 5 B

6 2 0 Z

6 4 0 B

6 4 0 Z

H 0 4 L 9/00

6 7 5 D

審査請求 未請求 請求項の数 9

O L

(全 11 頁)

(21) 出願番号 特願平10-145284

(22) 出願日 平成 10 年 (1998) 5 月 27 日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 榊原 裕之

東京都千代田区丸の内二丁目2番3号

三菱電機株式会社内

(72) 発明者 吉武 淳

東京都千代田区丸の内二丁目2番3号

三菱電機株式会社内

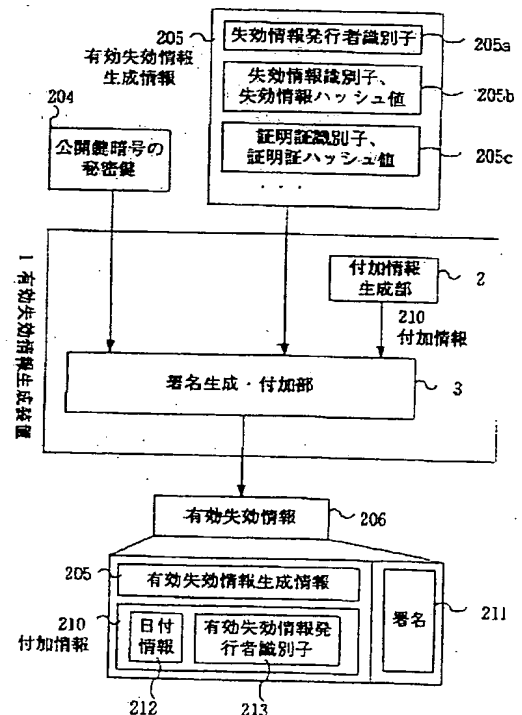
(74) 代理人 弁理士 宮田 金雄 (外2名)

(54) 【発明の名称】 失効情報検証方式

(57) 【要約】

【課題】 証明証が失効したことを示す失効情報を検証する処理を短縮することを目的とする。

【解決手段】 失効情報検証用の有効失効情報 206 の有効期限を示す日付情報 212 及び有効失効情報発行者識別子 213 で構成される付加情報 210 を生成する付加情報生成部 2 を備え、失効情報発行者の識別子 205 a と、失効情報の識別子 205 b と、失効情報ハッシュ値 205 b と、失効情報の署名を検証するための失効情報検証用証明証の識別子 205 c と、失効情報検証用証明証のハッシュ値 205 c とを連結した組みを 1 つ以上入力し、この入力データと付加情報生成部 2 により生成された付加情報 210 とを連結し、失効情報の管理機関が保持する公開鍵暗号の秘密鍵 204 による署名 211 を付加し、有効失効情報として生成する署名生成・付加部 3 をさらに備えた。



## 【特許請求の範囲】

【請求項 1】 以下の手段を備えた失効情報検証方式。

(a) 認証局により発行された証明証が失効したことを示す失効情報を検証するための有効失効情報の有効期限を示す日付情報と、上記有効失効情報の発行者を示す有効失効情報発行者識別子と、で構成される付加情報を生成する付加情報生成手段；

(b) 上記失効情報を発行した者の識別子と、上記失効情報の識別子と、上記失効情報を一方向性ハッシュ関数に入力して得た出力である失効情報ハッシュ値と、上記失効情報の署名を検証するための失効情報検証用証明証の識別子と、この失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力である証明証ハッシュ値とを連結した組みを 1 つ以上入力し、この入力データと上記付加情報生成手段により生成された付加情報とを連結し、上記失効情報の管理機関が保持する公開鍵暗号の秘密鍵による署名を付加し、上記有効失効情報として生成する署名生成・付加手段。

【請求項 2】 以下の手段を備えたことを特徴とする請求項 1 記載の失効情報検証方式。

(a) 上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

(b) 上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

(c) 上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報識別子を用いて該当する失効情報を取得する失効関連情報取得手段；

(d) 上記失効関連情報取得手段により取得した失効情報と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報取得時に用いた失効情報識別子を含む組の失効情報ハッシュ値とを比較し、この入力した失効情報の有効性を検証する有効性検証手段。

【請求項 3】 上記失効関連情報取得手段は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報識別子を用いて該当する各失効情報を取得することを特徴とする請求項 2 記載の失効情報検証方式。

【請求項 4】 上記失効関連情報取得手段は、上記失効情報識別子を入力し、この入力した識別子を用いて該当する失効情報を取得することを特徴とする請求項 2 記載の失効情報検証方式。

【請求項 5】 上記失効関連情報取得手段は、上記該当する失効情報を取得せずに、取得済みの失効情報を用い

ることを特徴とする請求項 2 記載の失効情報検証方式。

【請求項 6】 以下の手段を備えたことを特徴とする請求項 1 記載の失効情報検証方式。

(a) 上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

(b) 上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

(c) 上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する失効情報検証用証明証を取得する失効関連情報取得手段；

(d) 上記失効関連情報取得手段により取得した失効情報検証用証明証と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報検証用証明証取得時に用いた失効情報検証用証明証の識別子を含む組の証明証ハッシュ値とを比較し、この入力した失効情報検証用証明証の有効性を検証する有効性検証手段。

【請求項 7】 上記失効関連情報取得手段は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する各失効情報検証用証明証を取得することを特徴とする請求項 6 記載の失効情報検証方式。

【請求項 8】 上記失効関連情報取得手段は、上記失効情報検証用証明証の識別子を入力し、この入力した識別子を用いて該当する失効情報検証用証明証を取得することを特徴とする請求項 6 記載の失効情報検証方式。

【請求項 9】 上記失効関連情報取得手段は、上記該当する失効情報検証用証明証を取得せずに、取得済みの失効情報検証用証明証を用いることを特徴とする請求項 6 記載の失効情報検証方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、公開鍵暗号システムにおける公開鍵証明証の検証において、公開鍵証明証の失効情報を検証する方式に関するものである。

【0002】

【従来の技術】近年インターネット上での通信において、公開鍵暗号システムの利用が益々要求されている。公開鍵暗号システムを利用した安全な通信においては、認証局が発行した公開鍵証明証が必要となる。公開鍵証明証は、認証局が公開鍵とその持ち主の結びつきを認証局の公開鍵暗号の秘密鍵でデジタル署名を付加して証明したものである。公開鍵を安全に取得するために、公開

鍵は証明証パスと共に検証された公開鍵証明証から取得すべきである。証明証パスはある認証局により署名されたエンティティの証明証と、0個またはそれ以上の数の、別の認証局が発行した証明局の証明証から構成される。加えて、証明証パス上の証明証は失効してないことをチェックされなくてはならないので、認証局が発行する証明証で、有効期限が切れる前に失効したものをリストにしたCRLを失効のチェックに利用することは有効な手法である。

【0003】公開鍵証明証（以下、証明証という）の検証においては、認証局の証明証の発行形態と失効管理が検証の複雑さを左右する。証明証の発行、検証の方式としては、Network Working Group RFC1422 Privacy Enhancement for Internet Electronic Mail: Part 2: Certificate-Based Key Management, February 1993（文献1）や、Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extension Profile, NIST PKI-TWG March 9, 1998（文献2）に記載のX.509証明証の検証方式等が存在する。これらの方式では、X.509 ver1, ver3ベースの証明証における検証方法を述べている。

【0004】図4は、認証局の階層構造と証明証の発行形態を示す図であり、RFC1422（文献1）に示された証明証の発行方式を参考にした一例である。認証局（CA1）501、認証局（CA2）502、認証局（CA3）503は階層構造をなし、認証局（CA1）501は、自己署名証明証である証明証（Cert\_CA1）601を自分自身で発行し、さらに、認証局（CA2）502に証明証（Cert\_CA2）602を発行する。認証局（CA2）502は、認証局（CA3）503に証明証（Cert\_CA3）603を発行し、認証局（CA3）503は、UserA505に証明証（Cert\_UserA）604を発行する。なお、RFC1422（文献1）では、認証局（CA1）501に相当するIPRA（Internet Policy Registration Authority）は自身には証明証を発行せず自分の公開鍵のみを公開する。

【0005】次に、この様な、階層的な証明証の発行形態における各証明証の検証方式を説明する。証明証（Cert\_CA1）601を検証する場合は、認証局（CA1）501が自分自身に発行した自己署名証明証であるので、証明証（Cert\_CA1）601自身で検証可能である。証明証（Cert\_CA2）602を検証する場合は証明証（Cert\_CA1）601が必要になり、証明証（Cert\_CA3）603を検証する場合は証明証（Cert\_CA2）602が必要になり、証明証（Cert\_UserA）604を検証する場合は証明証（Cert\_CA3）603が必要になる。すなわち、この例では、証明証の検証は、信頼している最上位の認証局の証明証以外は上位の証明証が必要となる。証明証（Cert\_UserA）604を検証する場合は、証明証（Cert\_CA3）603、証明証（Cert\_CA2）602、証明証（Cert\_CA1）601を収集し、段階的に各証明証の正当性を検証しなくてはならない。これらの証明証の一連を証明証パ

スと呼ぶ。

【0006】図5は、図4において発行された証明証のパスを示す図であり、図5に示すように、各証明証には検証に必要な上位証明証の識別子が含まれている。例えば、証明証（Cert\_UserA）604においては、中に含まれるCert\_CA3\_IDが証明証（Cert\_CA3）603を指している。標準的な証明証である、X.509 ver3においては、この証明証の識別子の内容として、発行者Issuer、authorityKeyIdentifierが該当する。authorityKeyIdentifierは、上位の証明証に含まれるIssuerと通し番号（SerialNumber）、又は、keyIdentifierという上位の証明証に含まれる公開鍵に割り振られた一意な識別子である。従って、ある証明証を検証しようとした場合、その中を調べ、含まれている検証に必要な証明証の識別子をもとに、上位の証明証を収集し、その上位証明証に含まれる検証に必要な証明証の識別子をもとにさらに上位の証明証を収集するといった段階的な作業を必要とする。この例では、信頼している自己署名証明証である自分自身で検証が可能な最上位の認証局（CA1）501の証明証まで遡る必要があった。

【0007】さらに、各証明証について、上位の証明証に含まれる公開鍵で署名を検証した上で、持ち主、有効期限等の整合性の検証を行い、全ての証明証の整合性が確認できたなら証明証（Cert\_UserA）604を検証できたものとする。この例では、認証局（CA1）501が自身に証明証を発行し、検証者はこれを信頼し、この証明証にたどり着くまでパスを探しているが、自分が信頼している他の証明証まで遡るか、信頼する公開鍵で検証可能な証明証を指定してそこまで遡っても良い。RFC1422（文献1）では最上位の認証局（IPRA）は公開鍵のみを公開する。検証者はこの公開鍵を信頼できる手段で取得し、信頼した上で、一段下のPCA（Policy Certification Authority）の証明証までのパスを検証する。

【0008】証明証を上位の証明証を用いて段階的に検証することに加えて、認証局によっては、証明証の失効管理を行っている場合がある。図6は、図4において、各認証局が失効情報を発行していることを示す図であり、図6の例では、認証局がX.509のCertificate Revocation List (CRL)を発行している場合を示している。CRLは証明証が有効期限がきれる前に何らかの理由で失効したことを示す情報であり、認証局が発行した証明証で失効しているものの識別子をリストとして含み、認証局の公開鍵暗号の署名が付加されている。エンドエンティティであるUserA505が自分の証明証である証明証（Cert\_UserA）604を検証するためには、上述の証明証の段階的な検証に加えてCRLを利用して各証明証の失効をチェックする必要がある。

【0009】CRL（CRL\_CA1）611は、認証局（CA1）501が発行するCRLであり、認証局（CA1）501が失効を管理している証明証のチェック用に用いる。こ

の場合は、例えば、認証局 (CA2) 502 に発行している証明証 (Cert\_CA2) 602 及び証明証 (Cert\_CA2) 602 a の失効のチェックに用いる。同様に、CRL (CRL\_CA2) 612 は、認証局 (CA2) 502 が発行する CRL であり、認証局 (CA3) 503 に発行している証明証 (Cert\_CA3) 603 及び証明証 (Cert\_CA3) 603 a の失効のチェックに用いる。CRL (CRL\_CA3) 613 は、認証局 (CA3) 503 が発行する CRL であり、証明証 (Cert\_UserA) 604 の失効のチェックに用いる。なお、証明証 (Cert\_CA1) 601 a、証明証 (Cert\_CA2) 602 a、証明証 (Cert\_CA3) 603 a は、各々、CRL (CRL\_CA1) 611、CRL (CRL\_CA2) 612、CRL (CRL\_CA3) 613 の署名の検証に必要な公開鍵を含む証明証である。CRL は、各認証局が公開しており、UserA505 は各 CRL を取得する必要がある。

#### 【0010】

【発明が解決しようとする課題】従来の図 4 のような環境では、検証する証明証の上位の証明証を収集し、その中に含まれる検証に必要な上位の証明証の識別子を元にさらに上位証明証を収集するということを繰り返し、自己署名証明証にあたるまで収集を繰り返して証明証パスを形成する。そして、収集が終了したならば、収集した証明証を用いて、各証明証間の整合性の検証を行うという処理を行っていた。又は、検証する証明証の上位の証明証を収集し、2つの証明証間の整合性を検証し、それが成功したならば上位の証明証に含まれる検証に必要な上位の証明証の識別子を元にさらに上位証明証を収集し、2つの整合性を検証するということを繰り返し、自己署名証明証が見つかるまでくりかえすという処理を行っていた。これらの処理方式によれば、証明証の中の検証に必要な証明証識別子を調べて、上位証明証を収集するという作業は時間がかかるので、総合的にみると検証に時間がかかるという問題点があった。

【0011】加えて、認証局が失効管理をしている場合は、CRL 等の失効情報を利用し証明証の失効の確認をする必要があった。CRL の様に署名が存在する失効情報の検証においては、署名を検証するために認証局の証明証を必要とするが、この証明証に対しても証明証パスが生ずる。図 6 に示される証明証・CRL の発行形態において、図 7 に CRL (CRL\_CA3) 613 の署名を検証するための証明証パスを示す。CRL (CRL\_CA3) 613 の署名を検証するためには、署名を検証するための公開鍵を含む証明証 (Cert\_CA3) 603 a が必要であり、CRL (CRL\_CA3) 613 にはこれを示す識別子 Cert\_CA3 ID が含まれている。同様にして、証明証 (Cert\_CA3) 603 a を検証するためには、認証局 (CA1) 501 が認証局 (CA2) 502 に発行した証明証 (Cert\_CA2) 614 が必要であり、証明証 (Cert\_CA2) 614 を検証するためには、認証局 (CA1) が自身に発行した自己署名型の証明証である証明証 (Cert\_CA1) 6

15 が必要となる。

【0012】この CRL に関する証明証のパスである証明証 (Cert\_CA3) 603 a、証明証 (Cert\_CA2) 614、証明証 (Cert\_CA1) 615 と、図 5 における証明証 (Cert\_UserA) 604 に関するパスである証明証 (Cert\_CA3) 603、証明証 (Cert\_CA2) 602、証明証 (Cert\_CA1) 601 が同じ場合もあり、その場合は、証明証 (Cert\_CA3) 603 a と証明証 (Cert\_CA3) 603、証明証 (Cert\_CA2) 614 と証明証 (Cert\_CA2) 602、証明証 (Cert\_CA1) 615 と証明証 (Cert\_CA1) 601 が同一である。この場合は、パスの検証は一度で済む。しかし、認証局の運用によっては、各証明証が同一ではない場合があり、従って各パスが異なるケースが生じる。その場合は各パスについて、別々に署名を含めた検証を行わなくてはならない。図 6 の様に、複数の CRL が存在する場合に、各 CRL に関する証明証のパスについても同様で、悪い場合、調べなくてはいけない CRL の数分、証明証のパスが付加的に発生する。前述のように、証明証パスの収集、署名、項目の検証自体が時間のかかる処理であることに加え、失効情報の署名を確認するために、付加的な証明証のパスが発生し、本来検証したい証明証のパスの検証処理が大きくなるという問題点があった。

【0013】この発明は、上記のような問題点を解決するためになされたもので、ある証明証を検証するために発生した証明証パスにおいて、パス上の各証明証の失効状態を確認するのに必要な CRL 等の署名付き失効情報を検証する場合に、この情報に対して発生した証明証のパスの検証を簡略化することで、検証処理全体を短縮することを目的とする。

#### 【0014】

【課題を解決するための手段】請求項 1 の失効情報検証方式は、以下の手段を備えたものである。

(a) 認証局により発行された証明証が失効したことを示す失効情報を検証するための有効失効情報の有効期限を示す日付情報と、上記有効失効情報の発行者を示す有効失効情報発行者識別子と、で構成される付加情報を生成する付加情報生成手段；

(b) 上記失効情報を発行した者の識別子と、上記失効情報の識別子と、上記失効情報を一方向性ハッシュ関数に入力して得た出力である失効情報ハッシュ値と、上記失効情報の署名を検証するための失効情報検証用証明証の識別子と、この失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力である証明証ハッシュ値とを連結した組みを 1 つ以上入力し、この入力データと上記付加情報生成手段により生成された付加情報とを連結し、上記失効情報の管理機関が保持する公開鍵暗号の秘密鍵による署名を付加し、上記有効失効情報として生成する署名生成・付加手段。

【0015】請求項 2 の失効情報検証方式は、以下の手

段を備えたものである。

(a) 上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

(b) 上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

(c) 上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報識別子を用いて該当する失効情報を取得する失効関連情報取得手段；

(d) 上記失効関連情報取得手段により取得した失効情報と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報取得時に用いた失効情報識別子を含む組の失効情報ハッシュ値とを比較し、この入力した失効情報の有効性を検証する有効性検証手段。

【0016】請求項3の失効情報検証方式は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報識別子を用いて該当する各失効情報を取得する失効関連情報取得手段を備えたものである。

【0017】請求項4の失効情報検証方式は、上記失効情報識別子を入力し、この入力した識別子を用いて該当する失効情報を取得する失効関連情報取得手段を備えたものである。

【0018】請求項5の失効情報検証方式は、上記該当する失効情報を取得せずに、取得済みの失効情報を用いる失効関連情報取得手段を備えたものである。

【0019】請求項6の失効情報検証方式は、以下の手段を備えたものである。

(a) 上記管理機関の公開鍵に基づき、上記有効失効情報に付加された署名を検証する署名検証手段；

(b) 上記有効失効情報に含まれる付加情報を検証する付加情報検証手段；

(c) 上記失効情報を発行した者の識別子を入力し、この入力した識別子に一致する失効情報発行者識別子を上記有効失効情報より選別し、この選別した識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する失効情報検証用証明証を取得する失効関連情報取得手段；

(d) 上記失効関連情報取得手段により取得した失効情報検証用証明証と、上記署名検証手段及び上記付加情報検証手段により検証された有効失効情報とを入力し、この入力した失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力結果と、この入力した有効失効情報内の上記失効情報検証用証明証取得時に用いた失効情報検証用証明証の識別子を含む組の証明証ハッシュ値と

を比較し、この入力した失効情報検証用証明証の有効性を検証する有効性検証手段。

【0020】請求項7の失効情報検証方式は、上記失効情報を発行した者の識別子を複数入力し、この入力した各識別子に一致する失効情報発行者識別子を上記有効失効情報よりそれぞれ選別し、この選別した各識別子を含む組の上記失効情報検証用証明証の識別子を用いて該当する各失効情報検証用証明証を取得する失効関連情報取得手段を備えたものである。

10 【0021】請求項8の失効情報検証方式は、上記失効情報検証用証明証の識別子を入力し、この入力した識別子を用いて該当する失効情報検証用証明証を取得する失効関連情報取得手段を備えたものである。

【0022】請求項9の失効情報検証方式は、上記該当する失効情報検証用証明証を取得せずに、取得済みの失効情報検証用証明証を用いる失効関連情報取得手段を備えたものである。

【0023】

【発明の実施の形態】実施の形態1。以下の実施の形態では、証明証を発行する機関である複数の認証局があり、認証局が他の認証局、又はエンドエンティティに証明証を発行しており、加えてその証明証の失効に関する情報を公開鍵暗号の署名付きの失効情報として配布している環境で、ある証明証を検証する場合について説明する。なお、以下の実施の形態では、失効情報の一例として、X.509のCRLを取り扱う。図1は、この実施の形態における有効失効情報生成装置の構成図である。図において、1は失効情報の検証に用いるための有効失効情報を生成する有効失効情報生成装置、2は有効失効情報の有効期限を示す日付情報212と、この有効失効情報生成装置1の保有者の識別子である有効失効情報発行者識別子213とで構成される付加情報210を生成する付加情報生成部、3は付加情報210と有効失効情報生成情報205とを入力し、これらを連結し、この有効失効情報生成装置1を保有し、失効情報を管理する機関の公開鍵暗号の秘密鍵204を用いてこれに対して署名211を生成、付加し、有効失効情報206を生成した上で本生成装置の外部に出力する署名生成・付加部であり、有効失効情報生成装置1は、付加情報生成部2と署名生成・付加部3とから構成される。

40 【0024】有効失効情報生成情報205において、205aは失効情報の発行者の識別子である失効情報発行者識別子、205bは失効情報識別子、及び失効情報を一方向性ハッシュ関数に与えた結果である失効情報ハッシュ値を連結したもの、205cは失効情報の署名を検証するための公開鍵を含んだ証明証の識別子である証明証識別子、及び証明証を一方向性ハッシュ関数に与えた結果である証明証ハッシュ値を連結したものであり、この有効失効情報生成情報205は、失効情報発行者識別子205a、失効情報識別子及び失効情報ハッシュ値2

05b、証明証識別子及び証明証ハッシュ値205cの組み1つ以上で構成される。

【0025】図2は、この実施の形態における有効失効情報検証装置の構成図である。図において、4は、図1の有効失効情報生成装置1で生成された有効失効情報206を検証する有効失効情報検証装置であり、署名検証部5、付加情報検証部6、失効関連情報取得部7、有効性検証部8とにより構成される。208は有効失効情報206の署名211を検証するための公開鍵暗号の公開鍵であり、有効失効情報を管理する機関の公開鍵である。

【0026】署名検証部5は公開鍵208と有効失効情報206を入力とし、有効失効情報206の署名211を検証する。付加情報検証部6は、署名211の検証が済んだ有効失効情報206に記載されている日付情報212と有効失効情報発行者識別子213とを検証し、検証済み有効失効情報220を出力する。失効関連情報取得部7は、失効情報の発行者の識別子である失効情報発行者識別子207と検証済み有効失効情報220とを入力し、検証済み有効失効情報220に含まれている、失効情報発行者識別子207に該当する失効情報識別子221を判別する。加えて、失効情報識別子221を用いて装置外部から、該当する失効情報222を取得し、有効性検証部8に引き渡す。加えて、検証済み有効失効情報220に含まれている、失効情報発行者識別子207に該当する失効情報222の署名を検証するための公開鍵を含んだ証明証を示す識別子である証明証識別子223を判別し、これを用いて装置外部から該当する証明証224を取得し、有効性検証部8に引き渡す機能も有する。

【0027】有効性検証部8は、失効情報222と検証済み有効失効情報220とを入力し、検証済み有効失効情報220に含まれている失効情報222に該当する失効情報のハッシュ値を取り出し、これと失効情報222を一方方向性ハッシュ関数に入力した結果であるハッシュ値と比較し、一致を確認する。一致したならば、検証済み失効情報225として装置外部に出力し、一致しなかった場合はエラー情報227を出力する。加えて、証明証224を入力とし検証済み有効失効情報220に含まれる、証明証224に該当する証明証のハッシュ値を取り出し、証明証224のハッシュ値を生成して比較し一致を確認する。一致したならば、検証済み証明証226として装置外部に出力し、一致しなかった場合はエラー情報227を出力する機能を有する。

【0028】次に、図6の様に認証局が証明証・CRLを発行している環境で、図1に示した有効失効情報生成装置1の動作を図3に基づいて説明する。図3は、図1に示した有効失効情報生成装置1と、図2に示した有効失効情報検証装置4との関係を示すと共に、有効失効情報生成装置1による有効失効情報206の生成動作を説

明するための図である。図3において、認証局(CA1)101は、CA1の識別子CA1\_IDと失効情報CRL\_CA1をCA1の識別子及び失効情報201として失効情報管理機関104に渡し、認証局(CA2)102は、CA2の識別子CA2\_IDと失効情報CRL\_CA2をCA2の識別子及び失効情報202とし、認証局(CA3)103はCA3の識別子CA3\_IDと失効情報CRL\_CA3をCA3の識別子及び失効情報203として、失効情報管理機関104に渡す。各失効情報は最新のものを渡すこととする。

10 【0029】有効失効情報生成装置1を管理する失効情報管理機関104は、識別子及び失効情報203におけるCRL\_CA3の署名に関して証明証パスを生成する。これは、図7における、証明証(Cert\_CA3■)603a、証明証(Cert\_CA2■)614、証明証(Cert\_CA1■)615であり、これらに対し失効の検査を含めた必要な検証・検査を全て行い、正当性を検証した上で、証明証(Cert\_CA3■)603aに含まれる公開鍵を用いてCRL(CRL\_CA3)613の署名を検証する。検証に成功したならば、CRL(CRL\_CA3)613からCRL\_CA3の識別子を取り出し、CRL\_CA3\_IDとする。又、CRL(CRL\_CA3)613を一方方向性ハッシュ関数に入力した結果のハッシュ値をh(CRL\_CA3)とする。

【0030】さらに、CRL(CRL\_CA3)613の署名を検証するための公開鍵を含んだ証明証は証明証(Cert\_CA3■)603aであるが、証明証(Cert\_CA3■)603aの識別子をCert\_CA3■から取り出し、Cert\_CA3■\_IDとする。証明証(Cert\_CA3■)603aについても、一方方向性ハッシュ関数に入力し、結果のハッシュ値をh(Cert\_CA3■)とする。なお、証明証(Cert\_CA3■)603aはパスの検証において既に検証済みである。なお、205a3はCA3\_ID、205b3はCRL\_CA3\_IDとh(CRL\_CA3)の連結、205c3はCert\_CA3■\_IDとh(Cert\_CA3■)の連結である。

【0031】残りの認証局に関する失効情報も同様の操作を施し、これらを連結して有効失効情報生成情報205とする。すなわち、有効失効情報生成情報205は、CRL\_CA1に関する情報として、失効情報発行者識別子205aをあらわす205a1と、失効情報識別子及び失効情報ハッシュ値205bをあらわす205b1と、証明証識別子及び証明証ハッシュ値205cをあらわす205c1とを連結し、以下同様に、CRL\_CA2に関する情報として、205a2、205b2、205c2を連結し、CRL\_CA3に関する情報として、205a3、205b3、205c3を連結したものである。

【0032】即ち、図3に示した有効失効情報生成情報205の例は、図1に示した有効失効情報生成情報205を具体的に示すものであり、CRL\_CA1に関する情報は、205a1=CA1\_ID、205b1=CRL\_CA1\_ID.h(CRL\_CA1)、205c1=Cert\_CA1■\_ID.h(Cert\_CA1■)の連結であり、CRL\_CA2に関する情報は、205a2=CA2\_ID



D、205b2=CRL\_CA2\_ID,h(CRL\_CA2)、205c2=Cert\_CA2\_ID,h(Cert\_CA2)の連結であり、CRL\_CA3に関する情報は、205a3=CA3\_ID、205b3=CRL\_CA3\_ID,h(CRL\_CA3)、205c3=Cert\_CA3\_ID,h(Cert\_CA3)の連結であることを示している。

【0033】次に、図1に基づいて有効失効情報生成装置1の動作を説明する。有効失効情報生成装置1は、有効失効情報生成情報205と、失効情報管理機関104の公開鍵暗号の秘密鍵204とを入力し、有効失効情報206を生成する。有効失効情報205と秘密鍵204とを有効失効情報生成装置1が入力すると、付加情報生成部2は、有効失効情報206の有効期限等を表す日付情報212と、有効失効情報発行者識別子213とを連結し、付加情報210として出力する。署名生成・付加部3は、有効失効情報生成情報205と付加情報210とを連結した情報に、秘密鍵204を利用して署名211を付加し、有効失効情報206として出力する。即ち、有効失効情報206は、有効失効情報生成情報205と、日付情報212及び有効失効情報発行者識別子213から構成される付加情報210と、それらに対する署名211とから構成される。

【0034】次に、図6の様に認証局が証明証・CRLを発行している環境で、図2に示した有効失効情報検証装置4の動作を図3に基づいて説明する。図3において、UserA105は証明証の検証者であり、有効失効情報検証装置4を保持している。UserA105が自分の証明証(Cert\_UserA)604を検証する例を挙げる。UserA105は証明証(Cert\_UserA)604を検証するための証明証のパスを図5の様に生成する。すなわち、証明証(Cert\_UserA)604、証明証(Cert\_CA3)603、証明証(Cert\_CA2)602、証明証(Cert\_CA1)601を収集する。この時点で、証明証に含まれている情報から、失効情報であるCRLの発行者識別子を得ることができる。

【0035】例として、X.509では、証明証のSubjectが発行者識別子に該当する。すなわち、証明証(Cert\_CA3)603からはCRL\_CA3の発行者であるCA3の識別子CA3\_ID、証明証(Cert\_CA2)602からはCRL\_CA2の発行者であるCA2の識別子CA2\_ID、証明証(Cert\_CA1)601からはCRL\_CA1の発行者であるCA1の識別子CA1\_IDを得る。ここでは、CRL\_CA3の有効性を確認するために、有効失効情報206と、失効情報発行者識別子207としてCA3\_ID、失効情報管理機関104の公開鍵暗号の公開鍵208を有効失効情報検証装置4に入力する。公開鍵208については、有効失効情報206に含まれる付加情報210内の有効失効情報発行者の識別子213を調べ、この識別子213が示すエンティティが保持する公開鍵を入手する。

【0036】以降、有効失効情報検証装置4の動作を図2に基づいて説明する。署名検証部5は、有効失効情報

206と失効情報管理機関104の公開鍵208を入力とし、公開鍵208を利用して有効失効情報206の署名を検証する。署名に関するアルゴリズムは、有効失効情報生成装置1と同じ物を用いることとする。次に、付加情報検証部6は、有効失効情報206に含まれる日付情報212、有効失効情報の発行者識別子213で構成される付加情報210を検証し、有効期限などの日付情報が有効であるならば、検証済み有効失効情報220として出力する。

10 【0037】失効関連情報取得部7は、検証済み有効失効情報220を入力とし、さらに、装置外部から、有効性を確認したい失効情報の発行者識別子である失効情報発行者識別子207を入力とする。ここでは、認証局(CA3)103の発行した失効情報CRL\_CA3の有効性を確認するので、CA3\_IDを入力する。失効関連情報取得部7では、検証済み有効失効情報220に含まれている、有効失効情報生成情報205に該当する、CA1\_ID、CRL\_CA1\_ID、h(CRL\_CA1)、Cert\_CA1\_ID、h(Cert\_CA1)と、CA2\_ID、CRL\_CA2\_ID、h(CRL\_CA2)、Cert\_CA2\_ID、h(Cert\_CA2)と、CA3\_ID、CRL\_CA3\_ID、h(CRL\_CA3)、Cert\_CA3\_ID、h(Cert\_CA3)とから、CA3\_IDに該当する組を探し、発行している失効情報の識別子であるCRL\_CA3\_IDを取得する。これを失効情報識別子221として利用し、装置外部から該当する失効情報222を取得する。この場合は、CRL\_CA3が取得される。

20 【0038】次に、有効性検証部8は、外部から取得した失効情報222であるCRL\_CA3と検証済み有効失効情報220を入力とし、CRL\_CA3を一方方向性ハッシュ関数に入力しハッシュ値を計算する。一方方向性ハッシュ関数のアルゴリズムは、有効失効情報生成装置1と同じものとする。計算した値をh(CRL\_CA3)とする。有効性検証部8は、CRL\_CA3からCRL\_CA3\_IDを取り出し、これを利用して検証済み有効失効情報220に含まれる有効失効情報生成情報205に該当する情報からh(CRL\_CA3)を取り出し、h(CRL\_CA3)と比較する。一致すれば、検証済み失効情報225として出力し、一致しなければ、エラー情報227を出力する。取得したCRL\_CA3に対して計算したハッシュ値と、署名211と付加情報210を検証済みの検証済み有効失効情報220に含まれるハッシュ値が一致したということは、取得したCRL\_CA3は、失効情報管理機関104が署名を検証した上で有効失効情報206に記載したCRL\_CA3の識別子(CRL\_CA3\_ID)が示すものと一致することを意味する。すなわち、失効情報管理機関104が代理で署名の検証を行った失効情報を得たことになる。

40 【0039】従って、検証者であるUserA105は出力されたCRL\_CA1の署名を検証する必要はないので、CRL\_CA1の署名に関する証明証のパスも発生しない。ハッシュ値が一致しなかった場合、装置が偽造されたCRL\_CA3を取得した可能性があるため、エラーにする。他の失効情

報に関しても同様の操作で、検証済み失効情報として利用することができる。署名の検証に利用する失効情報管理機関の公開鍵は、信頼できる方法で取得したものを利用する。

【0040】実施の形態2。実施の形態1の有効失効情報検証装置は、検証済み失効情報の出力を行ったが、本実施の形態では、失効情報の署名を検証するための公開鍵を含んだ証明証の有効性を調べる場合について説明する。

【0041】図2において、検証済み有効失効情報220が生成されるまでの動作は実施の形態1に同様である。失効関連情報取得部7は、検証済み有効失効情報220を入力とし、加えて装置外部から、取得したい失効情報の発行者識別子である失効情報発行者識別子207を入力とする。ここでは、認証局(CA3)103の発行した失効情報CRL\_CA3を取得するので、CA3\_IDを入力とする。失効関連情報取得部7では、検証済み有効失効情報220に含まれている、有効失効情報生成情報205に該当する、CA1\_ID、CRL\_CA1\_ID、h(CRL\_CA1)、Cert\_CA1\_ID、h(Cert\_CA1\_ID)と、CA2\_ID、CRL\_CA2\_ID、h(CRL\_CA2)、Cert\_CA2\_ID、h(Cert\_CA2\_ID)と、CA3\_ID、CRL\_CA3\_ID、h(CRL\_CA3)、Cert\_CA3\_ID、h(Cert\_CA3\_ID)とから、CA3\_IDに該当する組を探し、失効情報を検証するための証明証の識別子であるCert\_CA3\_IDを取得する。これを証明証識別子223として利用し、装置外部から該当する証明証224を取得する。この場合は、Cert\_CA3\_IDが取得される。

【0042】次に、有効性検証部8は、外部から取得した証明証224であるCert\_CA3\_IDと検証済み有効失効情報220を入力とし、Cert\_CA3\_IDを一方方向性ハッシュ関数に入力しハッシュ値を計算する。一方方向性ハッシュ関数のアルゴリズムは、有効失効情報生成装置1と同じものとする。計算した値をh(Cert\_CA3\_ID)とする。有効性検証部8は、Cert\_CA3\_IDからCert\_CA3\_IDを取り出し、これを利用して検証済み有効失効情報220に含まれる有効失効情報生成情報205に該当する情報からh(Cert\_CA3\_ID)を取り出し、h(Cert\_CA3\_ID)と比較する。一致すれば、検証済み証明証226として出力し、一致しなければ、エラー情報227を出力する。実施の形態1と同様の理由で、検証済み証明証226の署名に関する検証はおこなう必要がないので、この署名に関する証明証のパスは発生しない。又、ハッシュ値が一致しなかった場合、装置が偽造されたCert\_CA3\_IDを取得した可能性があるため、エラーにする。UserA105は検証済み証明証226であるCert\_CA3\_IDを用いて、CRL\_CA3の署名を検証する必要がある。本実施の形態では、CRL\_CA3を既に取得していて、失効情報の署名を検証するための公開鍵を含んだ証明証を取得したい場合に有効である。

【0043】実施の形態3。実施の形態1の有効失効情

報検証装置4においては、失効情報者識別子をCA3\_ID1つだけに設定したが、CA3\_ID、CA2\_ID、CA1\_IDを連結して設定した場合は、検証済み有効失効情報220を生成した後で、失効関連情報取得部7はCA3\_ID、CA2\_ID、CA1\_IDの順番に従い、失効情報識別子としてCRL\_CA3\_ID、CRL\_CA2\_ID、CRL\_CA1\_IDを用いて、装置外部から失効情報222としてCRL\_CA3、CRL\_CA2、CRL\_CA1を取得し、それぞれ、失効情報検証部8に渡し、実施の形態1の様に検証済み有効失効情報220に含まれるハッシュ値との比較を行い、検証済み失効情報225として出力する。つまり、複数の失効情報の有効性の確認においても、有効失効情報206に対して、署名検証部5における署名の検証と、付加情報検証部6における付加情報の検証を1回で済ませることも可能である。

【0044】実施の形態4。実施の形態2の有効失効情報検証装置4においては、失効情報者識別子をCA3\_ID1つだけに設定したが、CA3\_ID、CA2\_ID、CA1\_IDを連結して設定した場合は、検証済み有効失効情報220を生成した後で、失効関連情報取得部7はCA3\_ID、CA2\_ID、CA1\_IDの順番に従い、証明証識別子としてCert\_CA3\_ID、Cert\_CA2\_ID、Cert\_CA1\_IDを用いて、装置外部から証明証224としてCert\_CA3\_ID、Cert\_CA2\_ID、Cert\_CA1\_IDを取得し、それぞれ、失効情報検証部8に渡し、実施の形態2の様に検証済み有効失効情報220に含まれるハッシュ値との比較を行い、検証済み証明証226として出力する。つまり、複数の証明証の有効性の確認においても、有効失効情報206に対して、署名検証部5における署名の検証と、付加情報検証部6における付加情報の検証を1回で済ませることも可能である。

【0045】実施の形態5。実施の形態1の有効失効情報検証装置4においては、失効関連情報取得部7に対して、失効情報発行者識別子207を入力したが、失効情報識別子221が分かっている場合は、失効情報発行者識別子207の代わりに失効情報識別子221を入力することで、失効情報222を取得することも可能である。又、失効情報222を既に取得している場合は、失効関連情報取得部7に対してこれらの識別子は入力せず、失効情報222を直接入力とし、有効性検証部8に引き渡すことも可能である。

【0046】実施の形態6。実施の形態2の有効失効情報検証装置4においては、失効関連情報取得部7に対して、失効情報発行者識別子207を入力したが、失効情報222を検証するための公開鍵を含んだ証明証の識別子が分かっている場合は、失効情報発行者識別子207の代わりに証明証識別子223を入力することで、該当する証明証224を取得することも可能である。又、証明証224を既に取得している場合は、失効関連情報取得部7に対してこれらの識別子は入力せず、証明証224を直接入力とし、有効性検証部8に引き渡すことも可能である。

【0047】

【発明の効果】請求項1の発明によれば、証明証が失効したことを示す失効情報を検証するための有効失効情報として、有効失効情報の有効期限を示す日付情報と、上記有効失効情報の発行者を示す有効失効情報発行者識別子と、上記失効情報を発行した者の識別子と、上記失効情報の識別子と、上記失効情報を一方向性ハッシュ関数に入力して得た出力である失効情報ハッシュ値と、上記失効情報の署名を検証するための失効情報検証用証明証の識別子と、この失効情報検証用証明証を一方向性ハッシュ関数に入力して得た出力である証明証ハッシュ値と、を含む情報を作成し、上記失効情報の管理機関が保持する公開鍵暗号の秘密鍵による署名を付加するので、失効情報の検証処理を短縮することができる。

【0048】請求項2の発明によれば、有効失効情報に付加された失効情報管理機関の署名と付加情報とを検証し、その後、失効情報発行者識別子を利用し、有効失効情報で指定される失効情報を取得し、この取得した失効情報のハッシュ値と有効失効情報に含まれるハッシュ値とを比較し、取得した失効情報の有効性を検証することにより、失効情報の署名を直接検証することなく正当性を確認できるので、失効情報の署名検証のための証明証パスが発生せず、失効情報の検証処理を短縮することができる。

【0049】請求項3の発明によれば、有効性を確認したい失効情報が複数ある場合、有効失効情報検証装置に対してそれら失効情報の発行者識別子を、複数一度に入力した場合でも、有効失効情報の署名を1度検証するだけで、失効情報の識別子で指定される全ての失効情報を取得でき、加えて、それらの署名を直接検証することなく正当性を確認できるという効果がある。

【0050】請求項4の発明によれば、失効情報識別子が分かっている場合は、失効情報を発行した者の識別子の代わりに、失効情報識別子を入力し、失効情報を取得することにより、検証処理を簡略化することができる。

【0051】請求項5の発明によれば、失効情報を既に所持している場合は、失効情報を発行した者の識別子や、失効情報識別子を入力することなく、保持している失効情報を用いるので、検証処理をさらに簡略化することができる。

【0052】請求項6の発明によれば、有効失効情報に付加された失効情報管理機関の署名と付加情報とを検証し、その後、失効情報発行者識別子を利用し、有効失効情報で指定される失効情報検証用証明証を取得し、この取得した失効情報検証用証明証のハッシュ値と有効失効情報に含まれるハッシュ値とを比較し、取得した失効情報検証用証明証の有効性を検証することにより、失効情報検証用証明証の署名を直接検証することなく正当性を確認できるので、失効情報検証用証明証の署名検証のための証明証パスが発生せず、失効情報検証用証明証の検

証処理を短縮することができる。

【0053】請求項7の発明によれば、失効情報の署名を検証するための公開鍵を含んだ証明証が複数あり、有効性を確認したい場合、有効失効情報検証装置に対して、失効情報の発行者の識別子を、複数一度に入力した場合でも、有効失効情報の署名を1度検証するだけで、該当する証明証を全て取得でき、証明証の署名を直接検証することなく正当性を確認できるという効果がある。

【0054】請求項8の発明によれば、失効情報検証用証明証の識別子が分かっている場合は、失効情報を発行した者の識別子の代わりに、失効情報検証用証明証の識別子を入力し、失効情報検証用証明証を取得することにより、検証処理を簡略化することができる。

【0055】請求項9の発明によれば、証明証を既に所持している場合は、失効情報を発行した者の識別子や、失効情報検証用証明証の識別子を入力することなく、保持している失効情報検証用証明証を用いるので、検証処理をさらに簡略化することができる。

【図面の簡単な説明】

20 【図1】 本発明の実施の形態1における有効失効情報生成装置の構成を示す図である。

【図2】 本発明の実施の形態1における有効失効情報検証装置の構成を示す図である。

【図3】 有効失効情報生成装置及び有効失効情報検証装置の動作を説明するための図である。

【図4】 認証局の階層構造と証明証の発行形態を示す図である。

【図5】 図4において発行された証明証のパスを示す図である。

30 【図6】 図4において、各認証局が失効情報を発行していることを示す図である。

【図7】 署名付きの失効情報に関して証明証パスが存在することを示す図である。

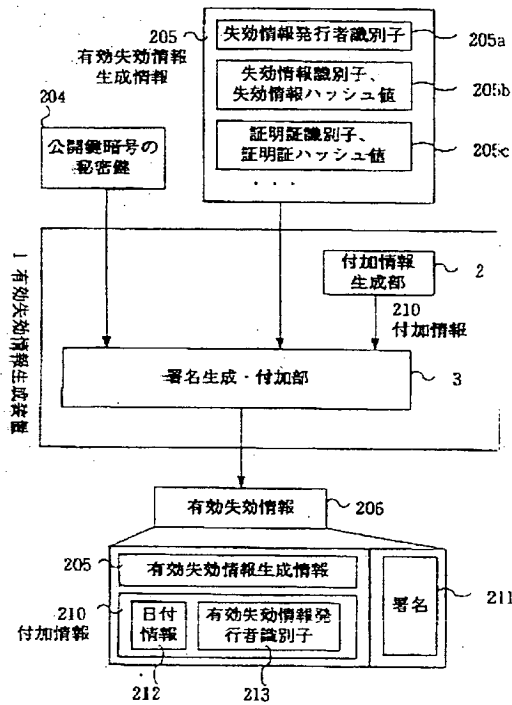
【符号の説明】

1 有効失効情報生成装置、2 付加情報生成部、3 署名生成・付加部、4 有効失効情報検証装置、5 署名検証部、6 付加情報検証部、7 失効関連情報取得部、8 有効性検証部、101 認証局(CA1)、102 認証局(CA2)、103 認証局(CA3)、104 失効情報管理機関、105 証明証の検証者であるUser A、201 CA1の識別子及び失効情報、202 CA2の識別子及び失効情報、203 CA3の識別子及び失効情報、204 秘密鍵、205 有効失効情報生成情報、205a 失効情報発行者識別子、205b 失効情報識別子及び失効情報ハッシュ値、205c 証明証識別子及び証明証ハッシュ値、206 有効失効情報、207 失効情報発行者識別子、208 公開鍵、210 付加情報、211 署名、212 日付情報、213 有効失効情報発行者識別子、220 検証済み有効失効情報、221 失効情報識別子、222 失効情報、2

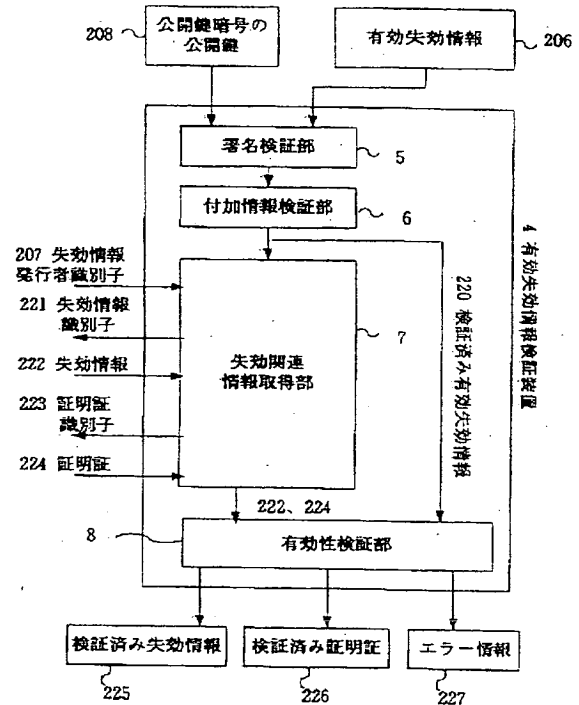
23 証明証識別子、224 証明証、225 検証済  
み失効情報、226 検証済み証明証、227 エラー

情報。

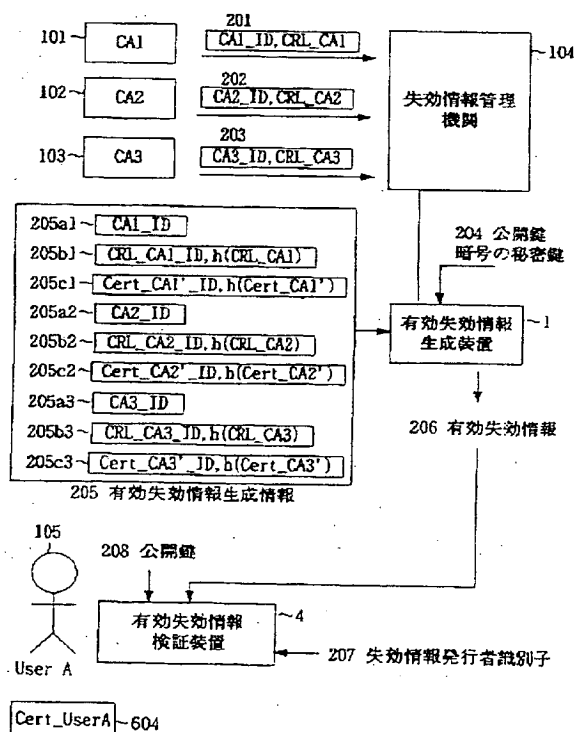
【図1】



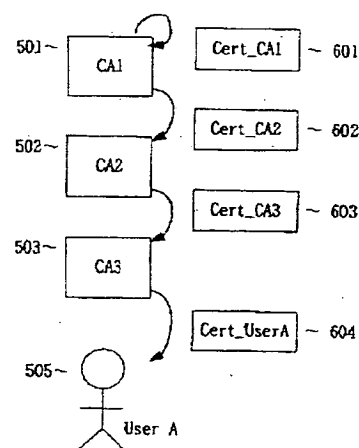
【図2】



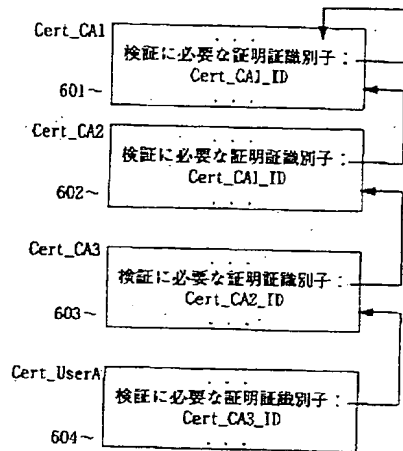
【図3】



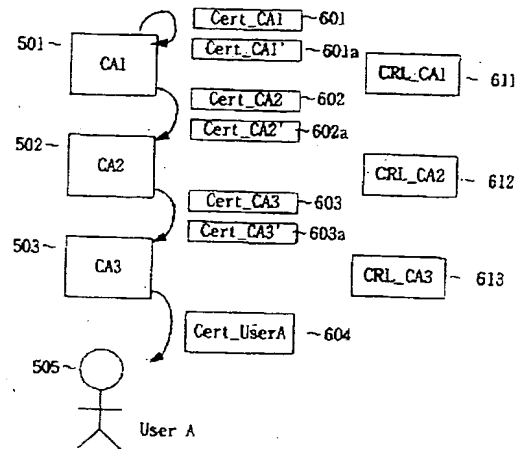
【図4】



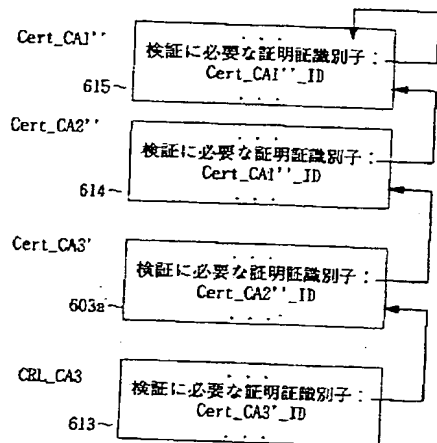
【図 5】



【図 6】



【図 7】



**THIS PAGE BLANK (USPTO)**